

**Studi Tentang Kriptografi Simetris:
Desain Algoritma *Block Cipher* dengan Skema
Transposisi pada Kubus Rubik**

Laporan Penelitian

**Diajukan kepada
Fakultas Teknologi Informasi
untuk Memperoleh Gelar Sarjana Komputer**



Peneliti:

**Vania Beatrice Liwandouw
(672012224)**

**Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Salatiga
Mei 2016**

**Studi Tentang Kriptografi Simetris:
Desain Algoritma *Block Cipher* dengan Skema
Transposisi Kubus Rubik**

Laporan Penelitian

Diajukan kepada
Fakultas Teknologi Informasi
untuk Memperoleh Gelar Sarjana Komputer



Peneliti:

**Vania Beatrice Liwandouw
(672012224)**

**Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Salatiga
Mei 2016**



PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama : VANIA BEATRICE LIWANDOUW
NIM : 672012224 Email : Vania.liwandouw@gmail.com
Fakultas : TEKNOLOGI INFORMASI Program Studi : TEKNIK INFORMATIKA
Judul tugas akhir : STUDI TENTANG KRIPTOGRAFI SIMETRIS : DESAIN ALGORITMA
BLOCK CIPHER DENGAN SKEMA TRANSPOSISI KUBUS RUBIK
Pembimbing : 1. ALZ DANNY WOWOR, S.Si., M.Cs
2. _____

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

Salatiga, 17 JUNI 2016



Tanda tangan & nama terang mahasiswa

Vania Beatrice Liwandouw



PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : VANIA BEATRICE LIWANDOUW
NIM : 672012224 Email : Vania.Liwandouw@gmail.com
Fakultas : TEKNOLOGI INFORMASI Program Studi : TEKNIK INFORMATIKA
Judul tugas akhir : STUDI TENTANG KRIPTOGRAFI SIMETRIS : DESAIN
ALGORITMA BLOCK CIPHER DENGAN SKEMA TRANSPOSISI
PADA KUBUS RUBIK

Dengan ini saya menyerahkan hak *non-eksklusif** kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

- ☒ a. Saya mengizinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA
- ☐ b. Saya tidak mengizinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA**

* Hak yang tidak terbatas hanya bagi satu pihak saja. Pengajar, peneliti, dan mahasiswa yang menyerahkan hak non-eksklusif kepada Repositori Perpustakaan Universitas saat mengumpulkan hasil karya mereka masih memiliki hak copyright atas karya tersebut.

** Hanya akan menampilkan halaman judul dan abstrak. Pilihan ini harus dilampiri dengan penjelasan/ alasan tertulis dari pembimbing TA dan diketahui oleh pimpinan fakultas (dekan/kaprodi).

Demikian pernyataan ini saya buat dengan sebenarnya.

Salatiga, 17 JUNI 2016

VANIA BEATRICE LIWANDOUW

Tanda tangan & nama terang mahasiswa

Mengetahui,

ALZ DANNY WOWOR

Tanda tangan & nama terang pembimbing I

Tanda tangan & nama terang pembimbing II

Lembar Persetujuan

Studi tentang Kriptografi Simetris : Desain Algoritma Block Cipher dengan Skema Transposisi Kubus Rubik

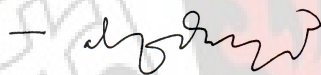
Laporan Penelitian

Peneliti:

Vania Beatrice Liwandouw (672012224)

Telah disetujui untuk diuji:

Tanggal: 10 JUNI 2016



Alz Danny Wowor, S.Si., M.Cs.

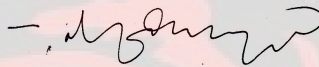
Pembimbing

1956

Lembar Pengesahan

Judul Tugas Akhir : Studi Tentang Kriptografi Simetris: Desain Algoritma *Block Cipher* dengan Skema Transposisi pada Kubus Rubik
Nama Mahasiswa : Vania Beatrice Liwandouw
NIM : 672012224
Program Studi : Teknik Informatika
Fakultas : Teknologi Informasi

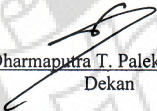
Menyetujui,



Alz Danny Wowor, S.Si., M.Cs.


Pembimbing

Mengesahkan,



Dr. Dharmaputra T. Palekahelu, M.Pd.

Dekan



Suprihadi, S.Si., M.Kom.

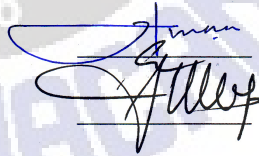
Ketua Program Studi

Dinyatakan Lulus Ujian tanggal: 10 Juni 2016

Penguji:

1. Prof. Ir. Danny Manongga, M.Sc., Ph.D.

2. Prof. Dr. Ir. Eko Sedyono, M.Kom



Bukankah telah Kuperintahkan kepadamu: kuatkan dan teguhkanlah hatimu? Janganlah kecut dan tawar hati, sebab TUHAN, Allahmu, menyertai engkau, ke manapun engkau pergi

Tulisan ini, ku persembahkan kepada Tuhan Yesus Kristus,
papa, mama, vika, viki, oma, dan orang yang kucintai.

vii

Kata Pengantar

Some people come in your life as blessings,
other come in your life as lessons. (Mother Theresa)

Penelitian teoritikal pada ranah fundamental merupakan studi yang dibutuhkan sebagai titik pijakan menuju pada kajian aplikatif. Pada ilmu komputer, algoritma menjadi *domain* yang penting untuk menjadi relasi dan fungsi menuju pada aplikasi berupa *tools (software)* yang menjadi *kodomain* ataupun *range*.

Studi algoritma kriptografi sebagai pijakan untuk merancang sebuah *tools* pengamanan informasi juga perlu dilakukan. Kebutuhan algoritma kriptografi mengalami transformasi sejak alat komunikasi yang digunakan manusia juga mengalami perubahan. Banyak studi yang lebih memperhatikan bagaimana merancang *tools* yang dapat diterapkan sebagai aplikasi *web* ataupun aplikasi *mobile* yang mendukung aktifitas manusia. Tetapi aplikatif akan menjadi sia-sia apabila kajian algoritma terhadap analisis kontekstual kekinian terutama kriptanalisis dan ruang kunci tidak diperhatikan.

Penelitian ini dilakukan memperhatikan aspek transposisi dan substitusi guna melihat faktor ruang kunci, yang menjadi ukuran peradaban perkembangan kriptografi pada saat ini. Oleh karena itu, penelitian yang dilakukan terdiri dari dua algoritma kriptografi dan dirancang berbasis pada kunci simetris dengan skema *block cipher*.

Algoritma pertama menekankan pada skema transposisi, kemudian dikembangkan pada penelitian kedua yang memperhatikan proses transposisi dan juga substitusi guna pemenuhan akan prinsip Shannon.

Kedua tulisan ini merupakan hasil kalaborasi dalam penelitian bersama Alz Danny Wowor yang dilakukan secara terpisah dan terpublikasi di seminar nasional pada tahun 2015. Penelitian pertama dengan judul “Desain Algoritma Berbasis Kubus Rubik dalam Perancangan Kriptografi Simetris” pada Seminar Teknik Informatika dan Sistem Informasi (SeTISI) di Universitas Kristen Maranatha, Bandung. Penelitian kedua yang berjudul “Kombinasi Algoritma Rubik, CSPRNG Chaos, dan S-Box Fungsi Linier dalam Perancangan Kriptografi Cipher Blok” dipublikasikan pada Seminar Nasional Sistem Informasi Indonesia (SESINDO) di Institut Teknologi Sepuluh Nopember Surabaya, dan berhasil terpilih sebagai *best paper* pada seminar nasional tersebut.

Laporan penelitian ini merangkum kedua penelitian yang diberikan pada bab yang berbeda. Sebagai pemenuhan akan *state of the art* maka sebagai pengantar yang diberikan pada bab pertama sebagai *general introduction* guna melihat masalah yang melatarbelakangi kedua penelitian ini. Setiap masalah dirangkum dalam sintesa-sintesa yang terjawab secara khusus diberikan pada bagian kedua dan bagian ketiga. Simpulan pada bagian terakhir dibuat menjadi sebuah *general discussion*. Bagian ini mencoba

membahas sintesa yang ada pada bagian awal sebagai simpulan dari kedua penelitian yang dilakukan.

Penelitian yang dilakukan dan tertuang dalam tulisan dengan format laporan penelitian ini, dapat dibuat dan terselesaikan hanya karena berkat dan tuntunan Tuhan Yesus Kristus. Tentunya juga atas dukungan serta doa dari orang-orang tercinta. Semoga tulisan ini dapat memberikan kontribusi dalam ranah algoritma kriptografi simetris. Sangat disadari bahwa tulisan ini merupakan embrio yang sedang berkembang menuju dan berjalan pada perbaikan yang masih jauh dari kesempurnaan, oleh karena itu berbagai kritik dan saran sangat diharapkan dan akan diterima dengan baik. Akhir kata, kiranya skripsi ini dapat bermanfaat dan berguna untuk kemajuan ilmu pengetahuan di masa yang akan datang. Tuhan Memberkati.

Salatiga, Juni 2016

Vania Beatrice Liwandouw

Abstrak

Kriptografi simetris khususnya block cipher sebagai sebuah algoritma pengamanan informasi memiliki keunggulan dari sisi efisiensi waktu dan dapat diimplementasikan di semua platform. Penelitian ini melakukan studi tentang block cipher khususnya proses transposisi menggunakan kubus rubik $4 \times 4 \times 4$. Selain transposisi, studi ini memperhatikan proses substitusi dan ruang kunci sebagai ukuran kompleksitas waktu yang diperlukan.

Metode transposisi yang dirancang pada kubus rubik $4 \times 4 \times 4$ sebagai media untuk menempatkan bit pada setiap sisi kubus rubik, sehingga total bit dalam sebuah kubus adalah 384 bit. Transposisi unik hasil dari perputaran yang dilakukan secara horizontal dan vertikal memberikan cipherteks yang secara grafik sangat fluktuatif. Kondisi ini menunjukkan algoritma yang dirancang memberikan efek diffusion antara plainteks dan cipherteks.

Studi selanjutnya menambah proses substitusi untuk melengkapi pemenuhan prinsip confusion. Fokus hanya pada satu bagian yaitu keacakan tidaklah cukup dalam rancangan algoritma kriptografi, sebab transposisi hanya merubah posisi objek dan tidak merubah nilai. Kombinasi transposisi dan substitusi mampu membuat algoritma dapat memenuhi prinsip Shannon, dan mengatasi uji ekstim. Selain itu untuk memperbesar ruang kunci, dilakukan pembangkitan kunci dengan CSPNRG berbasis Chaos.

Studi kriptografi simetris terkait desain algoritma blok cipher dengan Skema Transposisi pada Kubus Rubik memenuhi prinsip Shannon, lolos uji kunci lemah, S-Box, dan Iterated Cipher. Selain itu, penggunaan ruang kunci 384 bit akan menyulitkan kriptanalisis untuk melakukan uji brute force attack, sehingga akan dapat menahan serangan exhaustive key search dengan teknologi saat ini. Berdasarkan hal tersebut, rancangan ini dapat direkomendasikan sebagai kriptosistem dalam pengamanan informasi pada tataran studi sebuah algoritma.

Keywords: *Kriptografi Simetris, Blok Cipher, Transposisi, Substitusi, CSPNRG Chaos, Kubus Rubik $4 \times 4 \times 4$.*

Daftar Isi

	Halaman
Halaman Judul	i
Pernyataan Tidak Plagiasi	iii
Pernyataan Persetujuan Akses	iv
Lembar Persetujuan Pembimbing	v
Lembar Pengesahan	vi
Motto dan Persembahan	vii
Kata Pengantar	viii
Abstrak	xi
Daftar Isi	xii
Daftar Tabel	xiv
Daftar Gambar	xv
Bab 1: <i>General Introduction</i>	1
Bab 2: Desain Algoritma Berbasis Kubus Rubik dalam Perancangan Kriptografi Simetris	5
2.1 Pendahuluan	5
2.2 Landasan Teori	10
2.2.1 Pengertian Kriptografi	10
2.2.2 Rubik	12
2.2.3 Sistem Kriptografi	14
2.2.4 Menghitung Keacakan	14
2.3 Metode Penelitian	18
2.4 Hasil dan Pembahasan	14
2.5 Kesimpulan	26
Bab 3: Kombinasi Algoritma Rubik, <i>CSPNRG Chaos</i>, dan <i>S-Box</i> Fungsi Linier dalam Perancangan Kriptografi <i>Block Cipher</i>	27
3.1 Pendahuluan	27
3.2 Kajian Pustaka	29
3.2.1 <i>CSPNRG</i> Berbasis <i>Chaos</i>	29

3.2.2	<i>S-Box</i>	30
3.2.3	<i>Block Cipher</i>	30
3.2.4	Rubik	31
3.2.5	Sistem Kriptografi	32
3.2.6	Korelasi	32
3.3	Metode Penelitian	33
3.4	Rancangan Kriptografi	35
3.4.1	Algoritma Rubik	36
3.4.2	Rancangan <i>S-Box</i> Fungsi Linier	37
3.4.3	Pembangkitan <i>CSPNRG Chaos</i>	37
3.4.4	Proses Enkripsi-Dekripsi	39
3.4.5	Analisa Rancangan Kriptografi	39
3.4.5.1	Analisa Proses Ekripsi-Dekripsi	39
3.4.5.2	Analisis Korelasi	41
3.4.5.3	Analisis Ruang Kunci	42
3.6	Simpulan	43
Bab 4:	<i>General Discussion</i>	44
4.1	Pengantar	44
4.2	Proses Transposisi	47
4.3	Proses Substitusi	48
4.4	Ruang Kunci	48
4.5	Pemenuhan Prinsip <i>Block Cipher</i>	49
4.6	Simpulan	50
	Daftar Pustaka	51

Daftar Tabel

	Halaman
Tabel 2.1 Penjelasan Tahapan Penelitian	16
Tabel 3.1 Penjelasan Tahapan Penelitian	34



Daftar Gambar

	Halaman
Gambar 2.1 Skema Enkripsi dan Dekripsi	11
Gambar 2.2 Macam - macam rubik	14
Gambar 2.3 Tahapan Penelitian	13
Gambar 2.4 Pengujian Kriptosistem	16
Gambar 2.5 Proses Enkripsi dan Dekripsi	18
Gambar 2.6 Proses Awal Rubik	20
Gambar 2.7 Grafik Hasil Kasus 1	22
Gambar 2.8 Grafik Hasil Kasus 2	23
Gambar 2.9 Grafik Hasil Dekripsi Kasus 2	24
Gambar 2.10 Grafik Perbandingan AES dan Rancangan	25
Gambar 3.1 Skema Enkripsi dan Dekripsi Blok Cipher	25
Gambar 3.2 Kubus Rubik 4×4×4	32
Gambar 3.3 Tahapan Penelitian	33
Gambar 3.4 Proses Enkripsi dan Dekripsi	35
Gambar 3.5 Enam Sisi pada <i>Cubies</i>	36
Gambar 3.6 Proses Akhir Rubik	36
Gambar 3.7 <i>S-Box</i> Fungsi Linier	37
Gambar 3.8 Pembangkitan <i>Chaos</i> dengan $r = 3,71113$	38
Gambar 3.9 Pembangkitan <i>Chaos</i> dengan $r = 3,71114$	38
Gambar 3.10 Contoh Pertama (Plainteks Bervariasi)	41
Gambar 3.11 Contoh Kedua Plainteks Karakter Sama	41